A Systems Modelling Framework for the Design of Integrated Process Control Systems

Lind, Morten

Publication date:
1983

Document Version
Publisher's PDF, also known as Version of record

RISØ-M-2409

A SYSTEMS MODELLING FRAMEWORK FOR THE DESIGN OF INTEGRATED PROCESS CONTROL SYSTEMS

Morten Lind

Abstract. The paper describes a systems modelling methodology, called multilevel flow modelling, or MFM, which aims at describing complex production plants as designs, i.e. as systems having goals, functions and equipment realizing these functions. The modelling concepts are based on thermodynamics and lead to a system description in terms of multiple levels of interrelated mass or energy flow structures. The paper discusses as a basis for the modelling framework the general properties of artifacts or designs, characterizes the complexity of production systems and defines the MFM concepts which allow a consistent specification of goals and functions of these systems as generated in the process design. A modelling example is given and the application of the models for the design of plant control strategies is outlined.

INIS Descriptors. AUTOMATION; CONTROL SYSTEMS; CONSERVATION LAWS; ENERGY BALANCE; FLOW MODELS; INDUSTRIAL PLANTS; MASS BALANCE; NUCLEAR POWER PLANTS; PLANNING; REACTOR OPERATION.

UDC 62-52 : 621.039.564

December 1983

Risø National Laboratory, DK-4000 Roskilde, Denmark

Presented at IASTED Symposium ACI 83 on Applied Control and Identification, 1983. Copenhagen, Denmark.
Revised reprint.

28 juni 1 juli
The Int. Ass. of Science and Techn. for Develop.
Applied Contr. and Identification.

ISBN 87-550-0977-8
ISSN 0418-6435

Risø repro 1983

TABLE OF CONTENTS

INTRODUCTION

Recent developments in the control of complex production plants such as power plants and chemical processing units indicate a trend towards integration of protection functions and control functions for normal operation, and an increased integration of production functions in the plant. This is the case for nuclear power plants where some vendors provide flexible control schemes which allow a graduated handling of plant disturbances to avoid the initiation of protective functions when not absolutely necessary. The increased effort towards the reduction of energy consumption in the process industries has led to the consideration of more complex equipment resulting in increased process interaction. This tendency indicates that the control and supervision problems previously associated with large complex systems as nuclear power plants also will be faced in other process industries in the future. The result of this development should be an increased concern for the problems of control of complex systems. These problems include both the proper planning of the plant control strategies, the allocation of control functions to the computer and the operator and the design of man-machine interfaces which provide adequate support to the operator in diagnosis and control.

The application of computers for control supports this development, but full advantage has not yet been taken of the information processing capability of the modern computer. One of the reasons for this has been the lack of an appropriate theoretical framework which allows the analysis of the total control problem in a complex production plant independently of the actual implementation. This includes the consideration of sequence control for start-up or shut-down of plant systems, protection systems, control functions for normal operation and the interface to the operator. In order to obtain real improvements in plant control it is necessary to consider all these aspects of plant control as parts of an integrated problem.

The paper will describe a multilevel systems modelling framework (MFM, multilevel flow modelling) developed by the present author which has a potential as a basis for design of overall control strategies for production plants. The main principle in the modelling is to describe the process to be controlled as a design, or as an artifact adapted to the environment, i.e. as a system having goals, functions and physical components realizing these functions. A modelling language based on mass and energy balances is used for modelling the plant. This approach leads to a structured way of dealing with the problem of designing integrated control systems as it identifies the control tasks to be solved to achieve, maintain and protect normal operation. Furthermore it also provides the basis for design of information systems for operator support in diagnosis.

THE SYSTEM REPRESENTED AS AN ARTIFACT

The aim of the MFM modelling method is to describe a production plant as an artifact or as a system designed to satisfy specified purposes. The implications of this aim have profound consequences both for the modelling concepts used, the information gathering processes implied in the modelling activity, the kinds of questions which can be put to the model and the nature of the answers which can be expected. In the following I will discuss in more detail the implications of adopting a design stance in modelling.

The nature of designs has been discussed by Simon (1981). Simon characterizes an artifact or a design as - an interface between an "inner" environment, the substance and organization of the artifact itself, and an "outer" environment, the surroundings in which it operates. If the inner environment is appropriate to the outer environment, or vice versa, the artifact will serve its intended purpose -. The separability of the inner and outer environments is the reason why we can consider artifacts

as organized in levels and can describe behaviour of the system from different perspectives. This point is elucidated by the following citation from op.cit. - the advantage of dividing the outer from the inner environment in studying an adaptive or artificial system is that we can often predict behaviour from knowledge of system goals and its outer environment, with only minimal assumption about the inner environment -. - Furthermore, quite different inner environments accomplish identical or similar goals in identical or similar outer environments -. System goals are determined by the outer environment whereas the constraints of the inner environment determine system capability i.e. the limits of adaptability to the outer environment.

THE SYSTEMS APPROACH AND THE MODELLING OF ARTIFACTS

Simon's characterization of artifacts is closely related to the top-down approach to design, the so-called systems approach. As artifacts are distinguished from natural non man made systems by realizing the intentions of a design agent, identification of design goals provides an important ingredient in their modelling. The true nature of artifacts is not captured if goals are left unspecified. Gregory (1979) has given the following description of the systems approach as a managerial procedure relying upon

- the identification of objectives (or goals) to be attained
- the specification of functions needed to achieve those objectives
- the quantification of performance in terms of output quality and value
- the specification of parts of the system needed and their interrelationship

- the optimal configuration to achieve the objectives given the environment, constraints and resources.

This description of the systems approach to design identifies the key concepts to be considered in modelling of system designs. Note that a clear distinction is made between systems functions and their performance. Functions can be realized without consideration to their performance and a distinction should be made between what a system does and how well it does it. The latter requires some quantitative measure of performance. As an example it is possible to consider the heat removal function in a nuclear power plant as an abstract object without considering how much heat is removed. The heat removal function provides a potential for heat removal. This systems approach to design leads naturally to a description of a system in terms of an abstraction hierarchy.

THE ABSTRACTION HIERARCHY

The properties of process plants can be described by using an abstraction hierarchy as shown in figure 1 (Rasmussen, 1979). This hierarchy provides a multiple view of the same system in that each level emphasizes certain selected aspects of system properties. Abstraction hierarchies are used as overall modelling frameworks within several problem areas related to the topic considered here. As examples could be mentioned Computer Aided Design (Eastman, 1978), System Theory (Mesarovic et al., 1970), and Artificial Intelligence (Sussman et al., 1980).

On the highest level of abstraction in figure 1, the level of functional purpose, the system is described by its purpose, i.e. in terms related to its interaction with the environment. On this level, a power plant would thus be described as an energy production system since this description is adequate for dealing with its interaction with the environment, which consists of the electric distribution network and the con-

LEVELS OF ABSTRACTION

FUNCTIONAL PURPOSE

Production flow models,
system objectives

ABSTRACT FUNCTION

Causal structure, mass, energy &
information flow topology, etc.

GENERALISED FUNCTIONS

"Standard" functions & processes,
control loops, heat transfer, etc.

PHYSICAL FUNCTIONS

Electrical, mechanical, chemical
processes of components and
equipment

PHYSICAL FORM

Physical appearance and anatomy,
material & form, locations, etc.

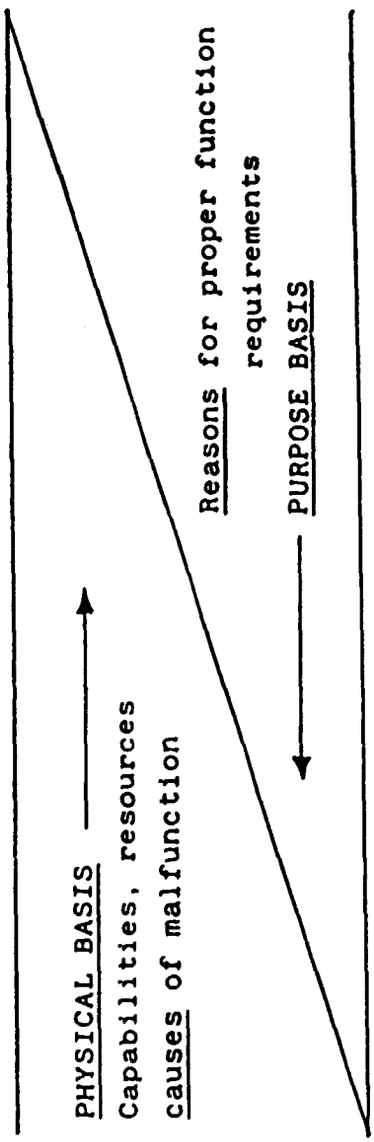

Fig. 1. The Abstraction Hierarchy for the description of technical systems.

sumers. When we shift a level down to the level of abstract function, we describe the internal function of the system in terms of the topology of the flow of energy, mass and information. This type of description represents the overall processes performed by the system considered and ignores physical details on how these processes are implemented. These details are described on the next lower levels. These types of models will be discussed in more detail below. Returning to the abstraction hierarchy in figure 1, the system can be described on the level of generalized function in terms of the behaviour of functionally integrated subsystems. In power plants, we can talk about the air-gas path in the boiler and the component cooling system etc. as abstract functional objects and the behaviour of the plant in terms of states of and interaction between these objects. In the example of a watch given by Sussman et al. (1980) this level provides a description in terms of balances, escapement and wheel-trains etc. Moving down to the level of physical function, the system is described in terms of interactions between components and equipment; i.e. valves, pumps, turbine generator units etc. This is the level which is usually described in a piping and instrumentation diagram. On the lowest level of abstraction we deal with the physical anatomy, material form and location in space.

The abstraction hierarchy organizes the different levels according to the degree with which they represent system properties related to the overall plant purpose or to the implementation in terms of physical components. At each level of abstraction, the reasons and specifications, i.e. the requirements for proper function, are formulated from above, and the means for control and potential for function, i.e. the physical capabilities and limitations, are coming up from below. In case of disturbances due to technical faults, the causes of malfunction are propagating bottom-up through the hierarchy of abstraction, at the same time as rules for proper functions are derived top-down.

CHARACTERISTICS OF SYSTEM COMPLEXITY

The notion of an abstraction hierarchy emphasizes the need of different levels of descriptions when modelling a technical system as a design. The complexity of designing and operating large processing units is partly due to the need of applying multiple perspectives on the system. But another factor which is important is the nature of relations between "objects" on different levels. Although we will deal in detail with these relations later it is appropriate to provide an idea of their nature already here.

Consider the overall production and safety goals of e.g. a nuclear power plant which are to maintain electricity production and to prevent the release of radioactive materials to the environment. Each of these goals can be approached by proper control of various functions related to inventory and heat balances in the plant system, and each function can in general be implemented by means of different equipment and configurations. Furthermore, each piece of equipment may support several plant functions. These many-to-many mappings (fig. 2) among the levels in the abstraction hierarchy contribute to system complexity. Control problems occur if several conflicting goals should be achieved by means of the same plant functions. But at the same time the many-to-many mappings also provide the potential for corrective actions by operators or automated controls, since they make it possible to replace a disturbed function by the service of other equipment. This reflects the use of redundancy or diversity techniques in the design for reliable and safe system operation.

There is, in addition to the many-to-many mappings discussed above, another type of relations between plant goals and functions which relates to the dynamic nature of systems. This is kind of equivalence relation dealing with cases where a goal specifies the function of a system with respect to its environment i.e. <u>what</u> it should do (not <u>how well</u>). Satisfaction of the goal requires the coordination of the functions of subsystems and takes time, hence the relation to dynamics. This

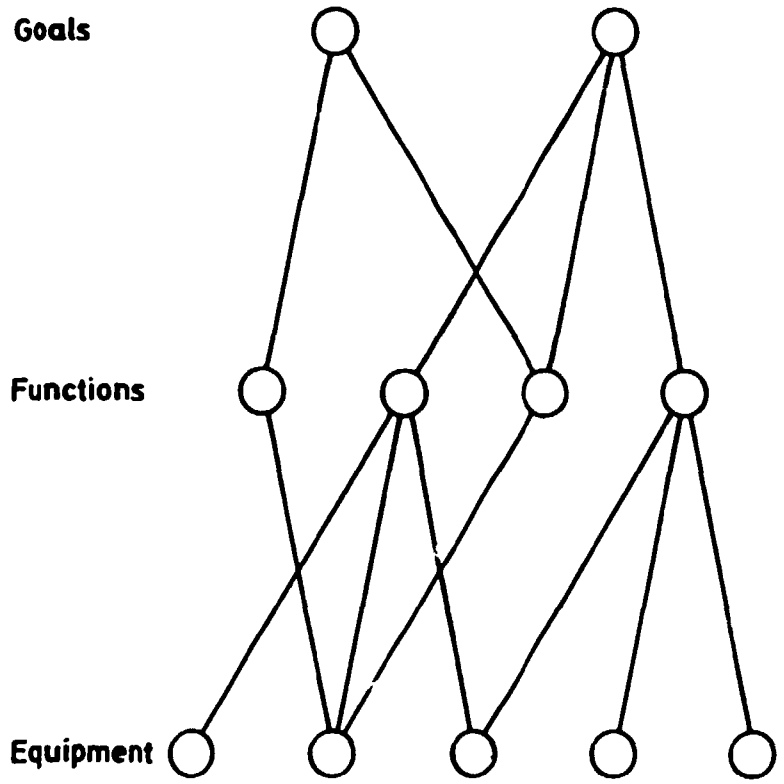

Fig. 2. System complexity is partly due to many-to-many mappings between goals, functions and equipment.

aspect is closely related to the recursive nature of the MFM models to be described later. The MFM approach allows the specification of system goals and functions using the same modelling concepts. The distinction between goals and functions depends on two interpretations of the model information.

Another factor contributing to complexity has to do with the conditions to be satisfied during plant operations in order to ensure proper system integrity and function. In terms of the distinction between goals, functions and equipment, there are three types of conditions. One relates to the conditions necessary to ensure that a certain plant function exists (this will be called a support condition), another type deals with

conditions necessary to ensure that the equipment (including its configuration) necessary for a certain plant function is available (an availability condition). The third type of condition deals with the situation where system reconfiguration is conditioned by the proper state of a plant function (a switching condition).

A consistent description of plant properties in a purpose - function - equipment hierarchy is accordingly an important basis for the design of overall plant control strategies involving the identification of control tasks and the subsequent allocation of tasks between operators and automated control and protection systems. This is a way to identify operational conflicts and constraints. Such a system description would at the same time provide a basis for design of operator support systems for diagnostic and supervisory purposes (Rasmussen and Lind, 1981). An approach to such a plant description has been made by Westinghouse (Rumancik et al., 1981) for the specification of a disturbance and surveillance system (DASS), and, in a more formal way, by Rasmussen (1979) and Lind (1979, 1981, 1982a and 1982c) the latter by the multilevel flow modelling methodology MFM to be described below.

MULTILEVEL FLOW MODELS

In multilevel flow modelling the functional structure of process plants is described in terms of a set of interrelated mass and energy flow structures on different levels of physical aggregation. The basic concepts used are closely related to thermodynamics which is the basis for every consistent approach to modelling physical phenomena in process plants. The methodology is used to provide normative models as the aim is to describe plant goals and functions as specified in the process design. The flow modelling concepts may also be used for descriptive purposes. A descriptive model represents the actual

behaviour of the system, whereas a normative model represents the system in terms of how it is intended to behave (Simon, 1981). This distinction is important for understanding how flow models are used for functional specification and for avoiding pitfalls in applying the methodology for this purpose. The modelling approaches in the two cases are basically different as the normative model requires a top-down function-oriented holistic approach whereas the descriptive modelling is a bottom-up atomistic approach starting with minute details and ending with a level of detail determined by simplifying assumptions. The MFM method distinguishes between two groups of modelling concepts, one related to the representation of plant goals and functions, the socalled flow functions, the other group deals with the representation of how flow functions are realized.

FLOW FUNCTIONS

The function of the plant and its subsystems is described in terms of a very restricted set of basic flow functions. These basic functions can be interconnected into functional networks called flow structures, such a network is also called a flow function. A flow structure is a functional network representing the plant on a level of physical detail given by an aggregation of plant components and equipment into subsystems. It is an important aspect of the methodology that this physical aggregation is motivated by functional considerations. Two distinct functional elements (nodes) in a flow structure may, as a result, correspond to two overlapping plant subsystems, i.e. they may share components. The individual functions will be explained below and their symbols used in the construction of flow structures are shown in fig. 3. The performance parameter mentioned in the explanations is a plant variable which can be used to evaluate the success of the system to perform its intended function.

- The storage function represents the property of a system to act as a buffer or accumulator of mass or energy. We distinguish between mass storage and energy storage. The storage function is characterized by a performance parameter indicating the amount of mass or energy accumulated.

- The transport function represents the property of a system to provide transfer of materials or energy between two other systems. As for the storage function, we distinguish between mass and energy transport. A transport function is characterized by a performance parameter indicating the rate of flow of the mass or energy transferred.

- The distributor function represents the property of a system to provide a balance between the total rates of incoming and outgoing flows. Again we distinguish between material and energy distribution. The performance parameter is a vector characterizing the ratios between rates of the individual ingoing/outgoing flows and the total ingoing/outgoing flows.

- The barrier function represents the property of a system to prevent the transfer of materials or energy between two other systems. We distinguish between material and energy barriers.

- The source/sink function represents the property of a system to benave as an infinite reservoir of mass or energy. No physically realizable system has in principle unlimited capability of delivering or receiving mass or energy. However, this representation may in many cases be perfectly adequate.

- The support function represents the property of a system to provide the conditions necessary to allow another system to perform its function. The performance parameter associated with a support function is the variable defined by the condition to be provided. The variable has no fixed type as it depends on the actual case. Any plant variable may be chosen such as e.g. temperature, pressure levels or flow variables.

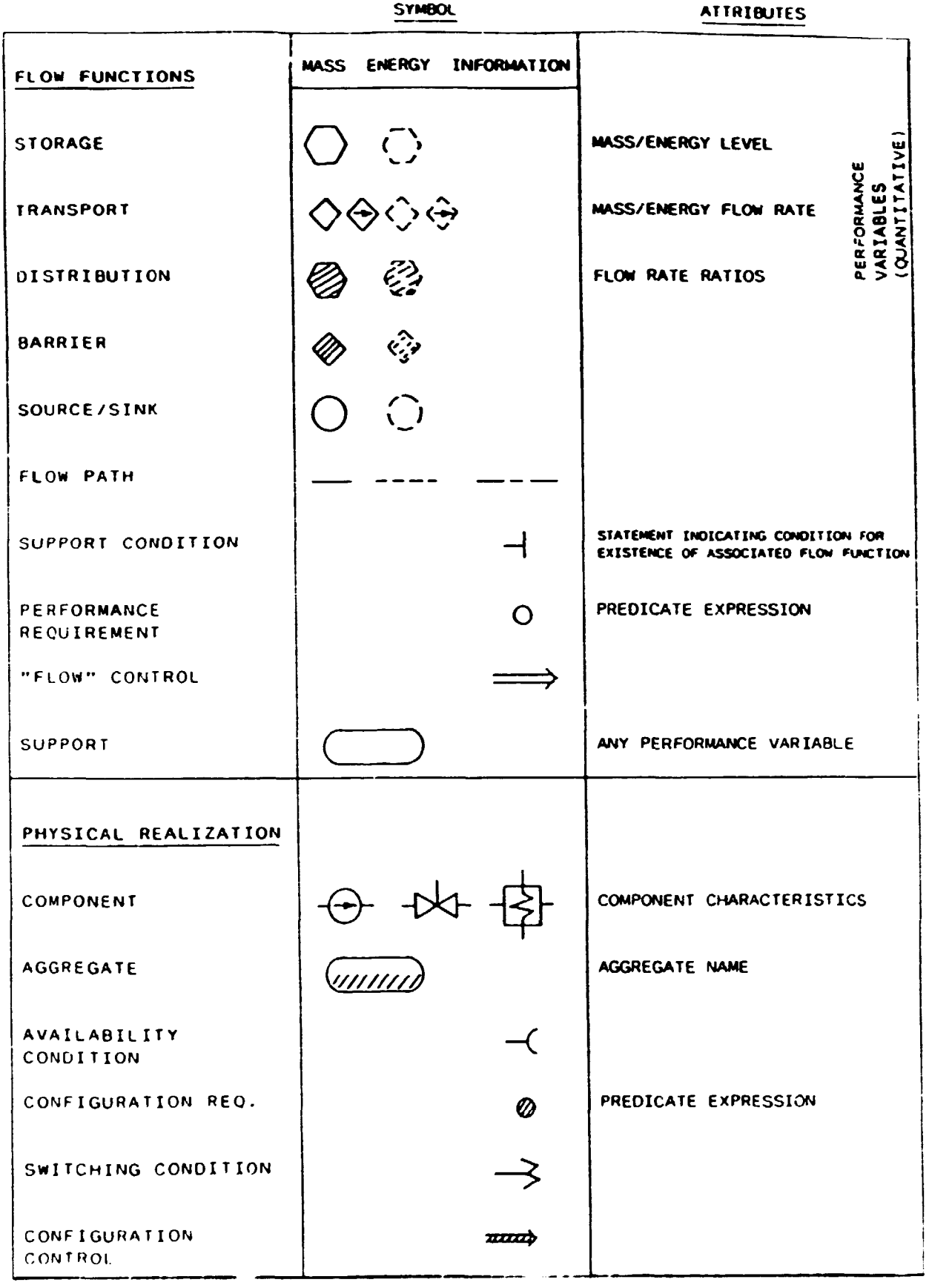

Fig. 3. Summary of Multilevel Flow Modelling concepts.

- A performance requirement represents a condition to be satisfied by performance parameters related to a flow function (any of the functions above). The requirement is expressed in terms of a predicate which should be true.

- A support condition describes the conditions to be satisfied in order to ensure that a flow function exists. Can be associated with any of the flow function above.

- Flow paths provide the linkage between the concepts above, mass flow paths interconnect mass flow functions, energy flow paths interconnect energy flow functions and information flow paths are used to interconnect conditions, performance requirements and support functions. It should be noted that flow paths are abstract concepts which do not have direct physical correlates such as pipes.

THE PHYSICAL REALIZATION OF SYSTEM FUNCTIONS

The modelling concepts above relate to the specification of goals and functions, i.e. they deal with a pure functional perspective and ignore how functions are realized. Now I will consider how to represent system implementation in terms of components, equipment and subsystems. In terms of the abstraction hierarchy this involves a description of the system on the level of physical function. As the choice of plant components and system configuration determines system capability, the description of system realization aspects deals with an important part of the representation of design decisions. The linkage of a flow function to its physical realization involves the following five modelling concepts.

- An availability condition identifies, in the form of a verbal statement, the system which should be available in order to provide the function in question. The condition can be considered as an attribute to the function.

- A specification of system goal configuration describes the component or subsystem interconnections which should be achieved, maintained or prevented in order to realize the function. For each goal configuration, the associated functional capability of the system may also be specified. This specification relates performance parameters of the function to parameters of system components.

- A physical aggregate identifies by name the system realizing the function (e.g. feedwater system, primary coolant circuit etc.) and its associated configuration parameters defining the degrees of freedom in configuring when realizing the function.

- A configuration control function represents the network switching task (valving) involved in the interconnection of a collection of components, equipments, or subsystems (physical aggregates) into an aggregate (as defined above). A valving procedure constitutes a specific solution to this task.

- A physical network is a network of components, equipment or subaggregates. The network represents the physical topology of the system realizing the function. Components are characterized by their functional characteristics.

- A switching condition describes a condition to be satisfied before equipment reconfiguration (interconnection, disconnection, closing or opening valves etc.).

It should be noted that a clear distinction is made between a support condition and an availability condition.

The formal similarity of these concepts with the flow concepts introduced previously should be noted. The similarity is due to the circumstance that the MFM method aims at the identification of control requirements in the plant. There is, from a formal point of view, no difference in specifying the task involved in the control of e.g. a plant subsystem temperature and the specification of system configuration. The logic structure is the same, only the content of the specifications will differ.

The problem spaces involved have the same form but have different "contents". In configuration control the network topology will define the system state whereas in temperature control the system state involved is a continuous variable.

A summary of the MFM modelling concepts as introduced above is given in fig. 3. This figure also indicates the symbols used in the construction of MFM models. Fig. 4 provides a simple example of how some of the concepts are used. Later I will describe a more elaborate example (see also Lind, 1982c).

DECOMPOSITION OF FLOW FUNCTIONS

The flow modelling framework described above can be used to describe plant function at any level of physical aggregation. This is possible because of the general nature of the thermodynamic conservation laws. In this way, we can describe a process plant from many perspectives or levels of abstraction using the same modelling concepts. As an example, we can describe a power plant on a high level as providing an energy distribution function, but we can also describe the plant on the level of pumps and valves. However, models on these two extremes of physical aggregation are related as the pumping function contributes to the overall plant function and because changes in requirements to overall plant performance (energy demand from grid) may lead to changes in the requirements on pump performance. These relations are established by proper decomposition of the flow functions in the overall plant model into lower level flow structures. This decomposition is guided by knowledge of the intentions of the plant designer. In principle any node in the flow structure can be decomposed, and the flow structures generated can again be decomposed leading to a recursive application of the modelling concepts. However, a distinction should be made between socalled vertical and horizontal decomposition.

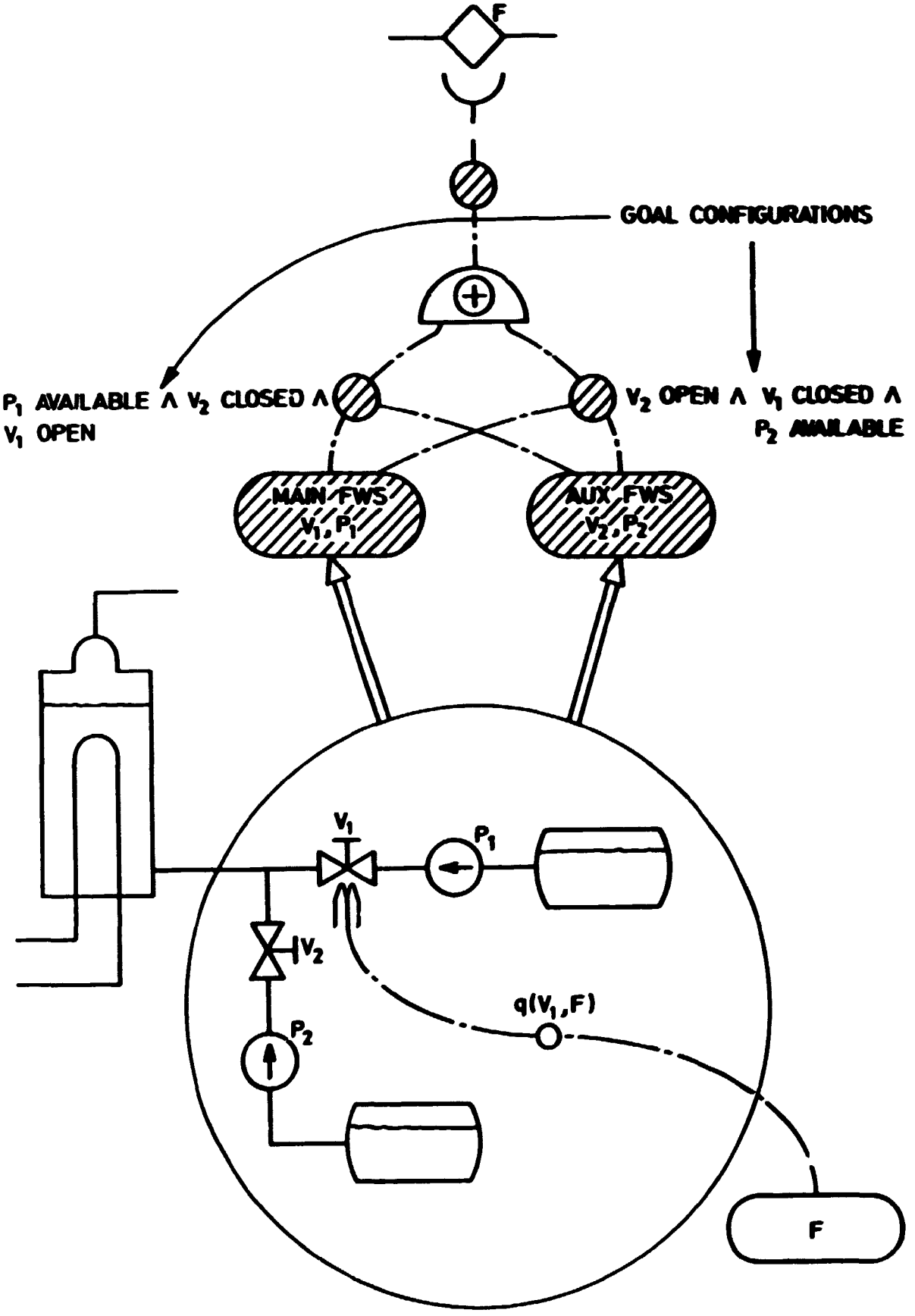

Fig. 4. Use of availability condition, configuration requirement, configuration control and aggregate concepts for the modelling of feedwater system realization.

In vertical decomposition, the model representing the decomposed flow function expresses the means available for the achievement of this function. A vertical decomposition leads to the description of the system on a lower functional level and corresponds in Simon's (1981) terminology to a transition from considering the "outer environment" to the description of the "inner environment". The use of vertical decomposition leads to the construction of multilevel flow models.

As an illustration of the use of vertical decomposition in flow modelling consider the example in Fig. 5. This example shows a model of a feedwater system consisting of a feed pump, a condensate pump and a feedwater tank. Two models are provided, on level 1 the feedwater system is described as a mass transport system, which indeed is the function intended of such a system. On level 2 the transport node on level 1 is decomposed into subfunctions including a flow control function, which in this case can be associated directly with the components of the system. This example shows a general aspect of a vertical decomposition that it increases the functional degrees of freedom. From considering only the flow F_1 on level 1 we consider two flows F_2 and F_3 and a mass M on level 2. This implies that F_2 and F_3 should be coordinated in order to ensure that the model on level 1 is an adequate description of the overall function of the feedwater system. We can accordingly consider the transport node on level 1 as specifying the goal of the function described on level 2, and the double arrow implies that a control function (automated or the manual) is required to constrain the variability on level 2. A possible constraint could be $F_1=F_2=F_3$. This corresponds to the choice of a specific control strategy and F_1 will be the setpoint for the resulting control loop. The aspects of vertical decomposition discussed here in terms of an example are general, i.e. flow functions can be considered as goals when decomposed and the decomposition implies a control constraint. However, when a support function is decomposed, the associated support condition is considered as the goal and not the support function itself.

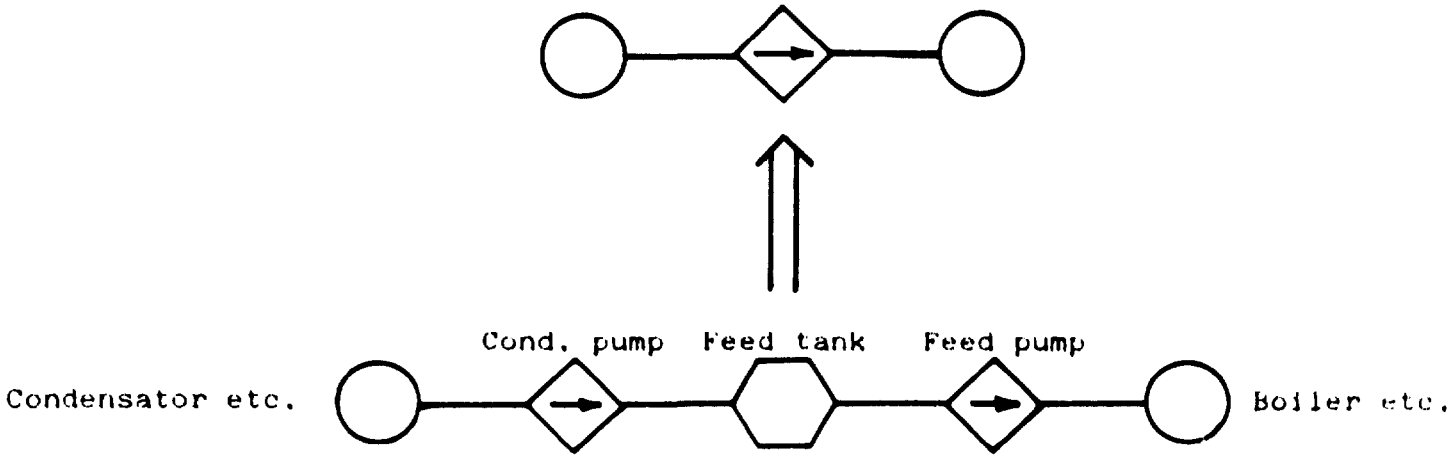

Fig. 5. Example illustrating the use of vertical decomposition in flow modelling.

When using horizontal decomposition a flow function is described in further detail without change of level. As an example could be given the decomposition of the mass transport node in fig. 5 on level 1 into two transport nodes in series. The function described by this decomposed model is essentially the same as for the original transport function.

The decomposition of a flow function cannot be done without considering how the function is realized and accordingly requires use of design information. In essence, the development of a multilevel flow model is a combined process of top-down decomposition of functions and a bottom-up aggregation of plant components and equipment into subsystems. The proper level of detail to apply in a plant model is determined by a matching of functions with physical aggregates. This may require an iterative process of both vertical and horizontal decompositions and physical aggregations before a successful match between functions and aggregates is obtained. One obstacle here is the fact that plant subsystems given names not always represent meaningful aggregates from a pure functional point of view. They may be chosen from other more pragmatic reasons.

In complex processing plants it is often the case that critical functions may be accomplished in several ways. As an example can be mentioned the main and the auxiliary feedwater systems in power plants as being alternative systems for the provision of feed flow to the steam generators. Similarly, a condition may be provided by several alternative support systems. Such alternatives can also be represented in a multilevel flow model. This is discussed in more detail in (Lind, 1982c).

From the discussion in relation to the example in fig. 5 it appeared that there are two interpretations of the information at any level in a multilevel model (Lind, 1982c) as the flow functions can be considered as specifying either goals or plant functions. This is an important aspect of the MFM modelling framework. The significance of this feature can be realized by considering three consecutive levels of vertical decomposition in a MFM model. Assuming that level i describes the function of a particular plant subsystem under investigation in a given

model application, then level i+1 will describe why this function is required. Similarly, level i-1 will describe how the plant function on level i is established and level i will relate to what is going on in the plant subsystems considered. The triple of why, what and hows can be shifted upwards or downwards as the subsystem considered changes and provides a systematic functionally motivated strategy for searching through model information. This may be important for the use of MFMs in training as it provides a way of organizing plant knowledge into a coherent structure. The why, what and hows are also important for an operator in diagnosis if supported by an information display designed on the basis of an MFM plant model (Goodstein, 1982a-b, Rasmussen and Lind, 1981). In constructing an MFM model it is also necessary to consider the triple as it guides the modeller in the choice of plant aspect to address at a given instant in the modelling (enforces the systems approach).

GENERIC CONTROL TASKS

From the discussion above it appears that in the MFM framework we can define a very restricted set of socalled generic control tasks. This is basically a consequence of using MFMs for functional specification. The highly structured and recursive nature of such models leads via the interpretation of the MFM as specifying control requirements to a considerable reduction in the number of control task categories to consider. The following generic types can be identified:

- maintain mass and energy inventories and flows at their target values or constraints.

- change mass and energy inventories to new target values or constraints.

- reconfiguration or network switching.

Any control task can be decomposed into sequences or concurrent sets of control tasks of the generic type. The concept of generic control tasks provides accordingly a useful tool for planning of complex control sequences. Another important property of generic control tasks is that they can be formulated within a uniform language which allows a consistent planning of control sequences which is independent of the actual physical context of the task. It could be an overall production control problem or it could be the problem in controlling lubrication oil flow to a pump.

To each generic control function in a MFM model a monitoring function is associated. Control functions allocated to the computer, i.e. all the automated controls, should be monitored by the plant operator. The monitoring requirement can readily be defined from the MFM model because the model specifies the control function which should be achieved, i.e. the goal of the control system, and sets accordingly the standard against which actual control system performance should be evaluated.

A MODELLING EXAMPLE

In order to illustrate the use of the MFM methodology, the modelling of a reactor coolant system will be discussed in some detail below. This example is chosen as it shows some of the main features of multilevel flow models and because it shows some characteristics of the functional structures of process plants. The physical realisation of the system function will not be modelled in detail, only the many-to-many nature of the relations between functions and equipment will be indicated. The coolant system and the multilevel flow model describing its functions are shown in figs. 6 and 7. But I will first, before discussing the model, describe the function of the reactor coolant system.

The reactor coolant system shown in fig. 6 is typical to pressurized water reactors (PWR) and is a very important system due to the safety concerns involved in its operation and because proper control of the system is also mandatory from the point of view of power production. Although the system (in this simplified version) has rather few components and looks simple, its functional structure is rather complex. This means that a description of the system at the physical level will not provide a proper understanding of its functional properties. This can be done in terms of an MFM model.

The purpose of the system is to transport energy from the reactor core to the steam generator secondary side where the heat is used to produce steam. The system has at the same time another purpose which is to act as a barrier for radioactive materials in order to prevent releases from the fuel to the environment. In order to function as a barrier it is required that temperatures and pressures are kept within specified limits. This involves the control of the energy accumulated in the system and of the water inventory. The pressure is controlled by management of the energy accumulated in the pressurizer. The transportation of energy through the coolant system is supported by the circulation of water in the coolant system. Flow of coolant water can be provided in two ways, by natural circulation (depending on temperatures in reactor core and steam generator primary side), or by forced circulation using a pump. The circulation will be prevented if system pressure decreases below the boiling pressure of the fluid because of boiling phenomena in the pump.

This description of the functional aspects of the coolant system was in fact a verbal description of the information in the MFM model of the system shown in fig. 7. From this model we can recognize the two overall goals of safety and production, and we can see how these goals/functions are supported by flow functions at lower functional levels down to the functional details of the pumping operation. It can be seen that the model is <u>not</u> a hierarchy because there are loops in the structure. Even when ignoring these loops the model is best characterized as two interconnected hierarchies. When taking the loops in

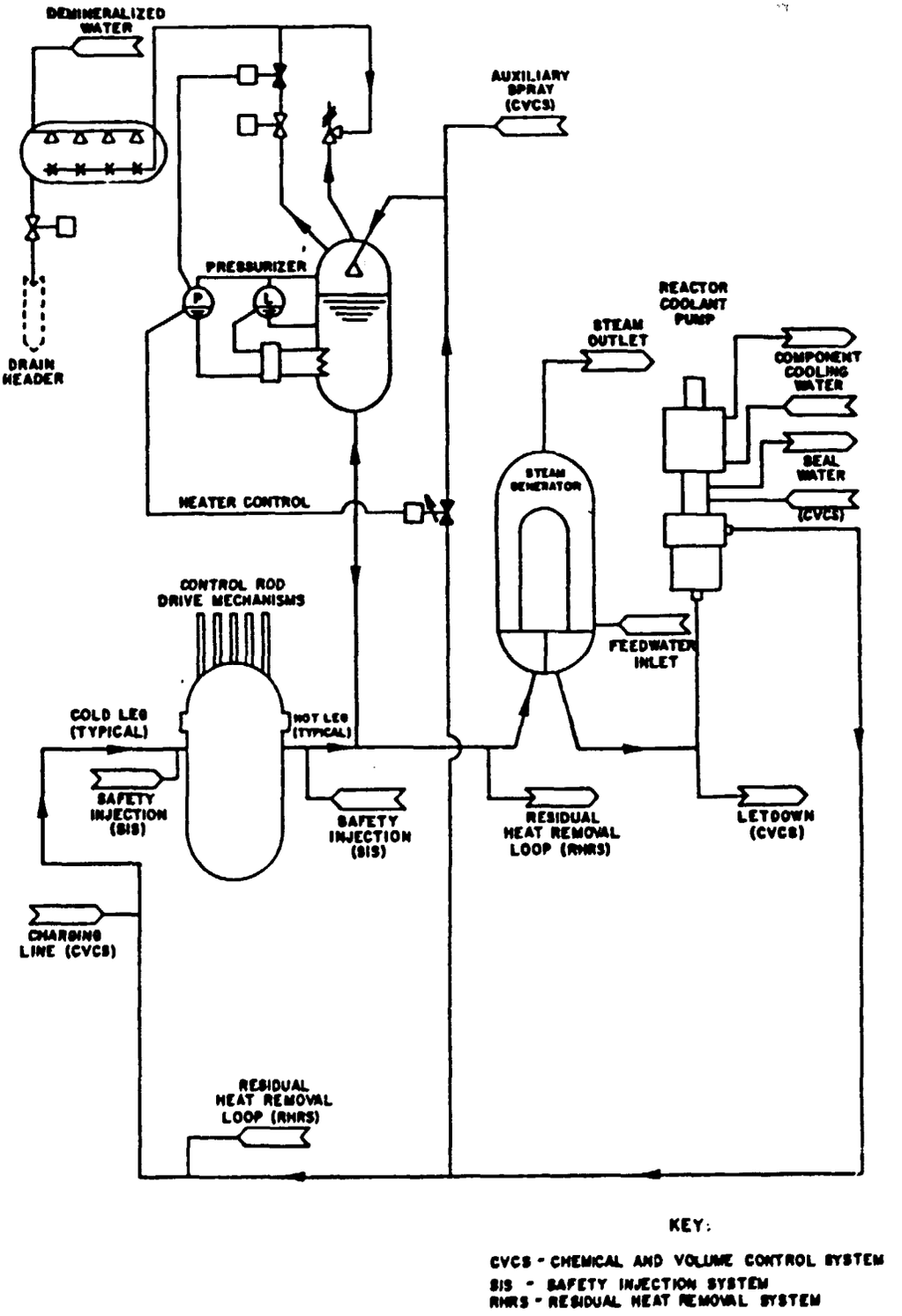

Fig. 6. Reactor coolant system modelled in Fig. 7.

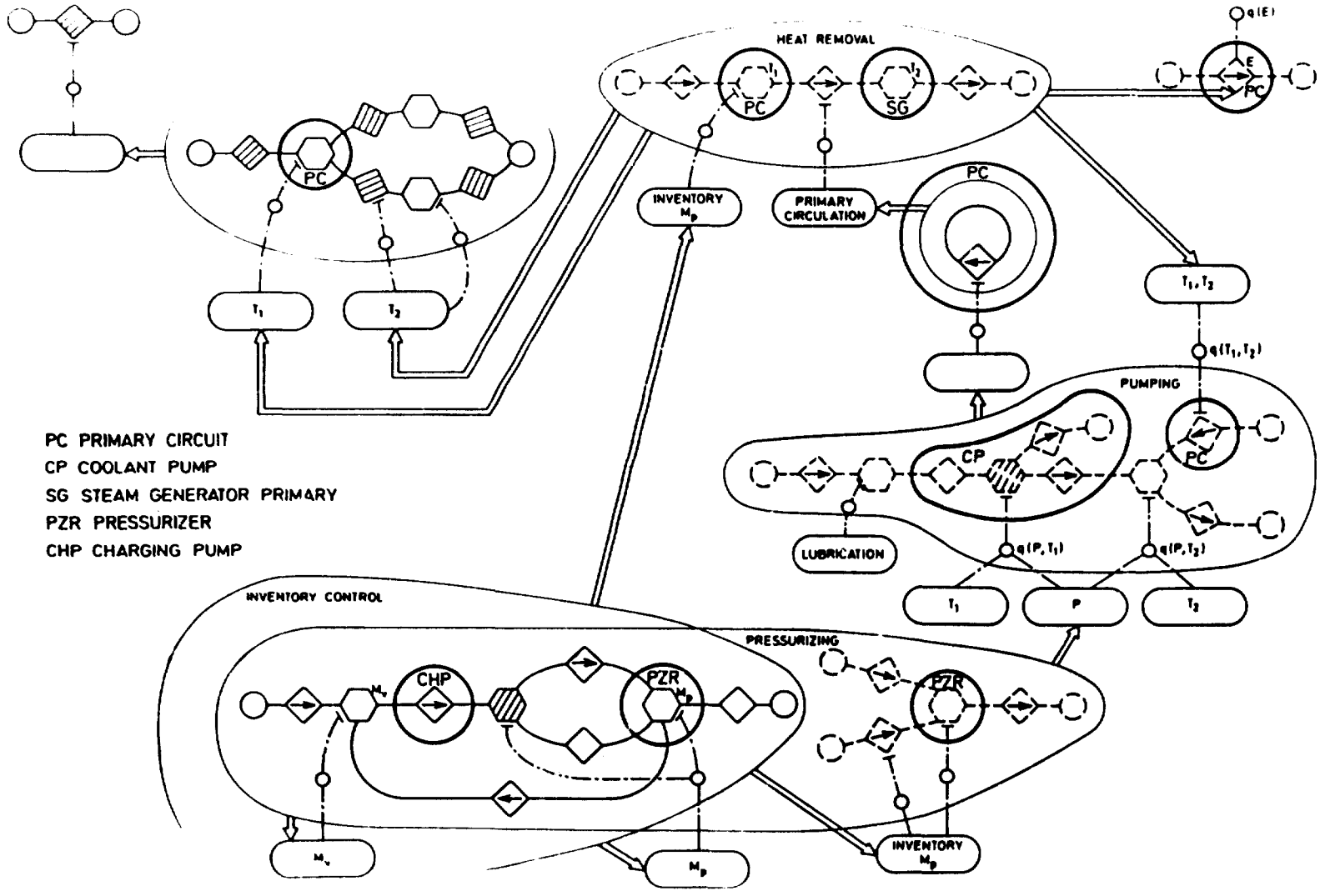

Fig. 7. Multilevel flow model of reactor coolant system.

consideration the model is a functional network. This will be the case for most MFM models. The appearance of loops in the structure indicates "bootstrapping" problems in the start-up of the coolant system. This problem is in the present case solved by providing alternative means of establishing pressure in the initial phases of the start-up. Loops will always indicate the need of auxiliary or "help" systems, and are important to identify in the planning of control strategies.

The nature of the many-to-many mappings between function and components can be seen in fig. 7 (heavy lines). Another interesting feature of the model is that support functions may provide conditions which relate to flow functions which are implemented by "subsystems" belonging to a level of physical decomposition which is below the level of components. This is the case for the pump in the example considered here. The pumping function is modelled by a (mechanical) energy balance, and a support condition at that level is provided by a high level plant function dealing with overall heat balance in the coolant system. These features are also general properties of multilevel flow models.

THE DESIGN OF CONTROL STRATEGIES USING MFMs

Multilevel flow models can be used as a basis for planning control strategies. The information in the model is created during process design and the modelling framework can be considered as a method of transferring process design information into control design. For this purpose it is important to recognize that an MFM model defines the problem space for decision making in control, i.e. it represents the total control problem to be handled by the control systems designer or the operator. This feature of MFM models is especially important when considering control problems where two or more goals should be pursued at the same time using the same plant functions and equipment. If one of these goals is related to

safety and has the highest priority the situation may call for a protective action. In other situations all goals may be reachable and lead to another control action. These two cases call for different control decision but the MFM framework allows the embedding of both decisions as two particular cases belonging to the same problem space. This is the reason why MFMs can be used as a basis for design of flexible control strategies.

The control synthesis problem considered includes both sequential automatics and continuous control, but does not deal with the actual control implementation which depends on the allocation of control tasks to the operator and the plant computer (Rasmussen & Lind, 1982). Rather, the approach deals with the control requirements as specified from plant design and the result of the synthesis is a scheduled plan of control tasks to be executed. Obviously, it is an assumption for the synthesis that the actual plant state and the goal to pursue have been properly identified in terms related to a plant MFM. This plant state identification problem has been discussed elsewhere (Lind, 1982b) and involves both the identification of the states of plant functions and the availability of equipment. The synthesis can, in principle, be divided into two separate phases, the first constitutes a planning phase resulting in a set of possible control strategies to apply, and the second is a scheduling phase in which the strategies developed during the planning phase are evaluated for feasibility, i.e. whether they actually can be carried out within the actual operational constraints. If a strategy is found not feasible another must be chosen or another goal should be pursued.

The planning phase deals with the functional relations as specified in the MFM for the given operating mode considered. Assuming a hierarchical model (i.e. no loops via conditions) we obtain readily a partial ordering of control tasks by considering the logic precedence of conditions in the model (equipment should be available before a function is realized, support condition should be satisfied before the function is operable and switching conditions satisfied before configuration changes). Accordingly the MFM can be used to derive a set of

sequence or concurrent sets of generic control tasks on the basis of plant state information, each sequence representing a possible strategy.

In the scheduling phase different categories of constraint information can be used to determine the feasible set of strategies. One type of constraint originates from the one-to-many and many-to-one relations between functions and physical structure as discussed previously. Generic tasks within the same control sequence may be related to plant functions which are mapped into the same physical subsystem. This makes the two control tasks dependent and requires coordination of control actions if the goals related to the two tasks should both be satisfied. This is the problem of decoupling in control theory. This type of constraints may in some cases render the whole associated control strategy inapplicable if alternative physical implementations of the functions involved are not available. In such a case a new strategy must be selected from the planning phase and evaluated. Another type of constraints which are used in the scheduling phase for discarding or selecting strategies are the resources of mass, energy, and time.

The generation of all possible plans as described above will not be a practical approach in most cases because a very large number of plans will usually be generated and a solution to the whole synthesis problem cannot be obtained. This is a general problem in design problems involving large solution spaces. A solution to this problem is to apply different heuristics to reduce the size of the solution space. These problems are not unique to the specific planning problem studied here. It has also been discussed in relation to robot problems within artificial intelligence research (Nilsson, 1980).

The synthesis procedure outlined above may be followed by the control system designer and the result being operating instructions to the operator and programs for automated control functions. The operator may also use the procedure for coping with unforeseen situations where operating instructions are not available. This will require extensive computer support and

changes of the man-machine interface as discussed in (Rasmussen & Lind, 1981) and changes of the content of training towards the emphasis of general problem solving skills. As a third possibility the synthesis procedure may be the basis for an adaptive or selforganizing control program.

APPLICATIONS OF THE MFM METHOD

An extensive application of the MFM methodology has been made by Westinghouse Electric Corporation, U.S.A., and Risø in cooperation. In this study, the MFM methodology was used as a systematic approach to the identification of critical safety and availability requirements of a nuclear power plant (PWR) as formulated by Westinghouse in the DASS/EPRI study (Rumancik et al., 1981). Results from this application of the MFM methodology have been published by De et al. (1982) and the work provide a basis for the development of a new advanced control room concept.

Another application of the MFM framework has been done in relation to the work of Goodstein (1982b) on the development of new display concepts and the GNP experimental program (Goodstein et al., 1983) for operator support evaluation. Part of this program will also consider the use of MFM plant models for training and for the design of knowledge-based systems for operator support in diagnosis. A related experimental program is conducted by the OECD Halden project (Yoshimura et al., 1983).

The modelling method will also be applied in risk assessment as a consistent way of specifying the context of operator decisions with the aim of identifying sources of human error which are due to the design of the operators task environment (Rasmussen et al., 1982).

ACKNOWLEDGEMENTS

This work is part of the joint Scandinavian NKA/LIT project on Human Reliability supported by the Nordic Council of Ministers.

The feedback received from users of the MFM methodology at Westinghouse and colleagues at Risø is greatly appreciated. With this information available, it has been easier to pinpoint the unprecise points and the aspects which needed further development.

REFERENCES

De, M.K. et al., "A Functional Design Approach to PWR Safety". Proc. of the International Meeting on Thermal Nuclear Reactor Safety held at Chicago, Illinois, U.S.A., August 29 - September 2, 1982. NUREG/CP-0027, pp. 1943-1957.

Eastman, C.M., "The Representation of Design Problems and Maintenance of Their Structure". IFIPS Working Conference on Application of AI and PR to CAD, Grenoble, France, March 1978.

Goodstein, L.P., "Computer Based Operating Aids". Paper presented at Design 1982 in Birmingham, September 1982a.

Goodstein, L.P. et al., "The GNP Test Bed for Operator Support Evaluation". Enlarged Halden Programme Group Meeting on Fuel Performance Experiments and Analysis and Computerized Man-Machine Communication, Loen, Norway, 23rd-28th May, 1983.

Goodstein, L.P., "An Integrated Display Set for Process Operators". Paper presented at the IFAC/IFIP/IFORS/IEA Conference on "Analysis, Design and Evaluation of Man-Machine Systems", Baden-Baden, F.R. Germany, September 27-29, 1982b.

Gregory, S.A., "Design Strategies and Tactics". Paper presented at ICE Symposium: Current Design Thinking, September 12-14, 1979, Aston University, England.

Lind, M., "The Use of Flow Models for Design of Plant Operating Procedures". Risø-M-2341. Paper presented at: IWG/NPPCI Specialists Meeting of Procedures and Systems for Assisting an Operator during Normal and Anomalous Nuclear Power Plant Operation Situations, December 5-7, 1979, Garching, F.R. Germany.

Lind, M., "The Use of Flow Models for Automated Plant Diagnosis". In: Rasmussen, J. and Rouse, W.B. (Eds.), "Human Detection and Diagnosis of System Failures". Plenum Press, New York, 1981.

Lind, M., "Artificial Intelligence Technique in Process Plant State Identification". Paper presented at: SAIS-82 Workshop on Artificial Intelligence, April 24-25, 1982b. UPMAIL Uppsala University, Sweden.

Lind, M., "Generic Control Tasks in Process Plant Operation". Paper presented at the 2nd European Annual Manual, Bonn, F.R. Germany, 1982a.

Lind, M., "Multilevel Flow Modelling of Process Plant for Diagnosis and Control". Proc. of the International Meeting on Thermal Nuclear Reactor Safety held at Chicago, Illinois, U.S.A., August 29 - September 2, 1982c. NUREG/CP--0027, pp. 1653-1666.

Mesarovic, M.D. et al., "Theory of Hierarchical Multilevel Systems". Academic Press (1970).

Nilsson, N.J., "Principles of Artificial Intelligence". Tioga Publ., U.S.A., 1980, 476 pp.

Rasmussen, J., "On the Structure of Knowledge - A Murphology of Mental Models in a Man-Machine System Context. Risø-M--2192, 1979.

Rasmussen, J. and M. Lind, "Coping with Complexity". Risø M--2293, 1982. Paper presented at European Annual Conference on Human Decision and Manual Control, Delft, 1981.

Rasmussen, J. and M. Lind, "A Model of Human Decision Making in Complex Systems and Its Use for Design of System Control Strategies". Proc. of the American Control Conference ACC-82, Arlington, U.S.A., pp. 270-276.

Rasmussen, J. et al., "Formalized Search Strategies for Human Risk Contributions. A Framework for Further Development". Risø-M-2351. July 1982.

Rumancik, J.A., "Establishing Goals and Functions for a Plant-Wide Disturbance Analysis and Surveillance System (DASS)". IEEE Trans. Nuclear Science, NS-28, No. 1, February 1981, pp. 905-913.

Simon, H.A., The Sciences of the Artificial. The MIT press, 2nd ed., 1981, pp. 247.

Sussman, G.J. and G.L. Steele Jr., "Constraints - A Language for Expressing Almost Hierarchical Description". Artificial Intelligence, Vol. 14, No. 1 (August 1980), pp. 1-40.

Yoshimura et al., "Development and Pilot Test of Multilevel Flow Modelling Displays Using the GNP". Enlarged Halden Programme Group Meeting on Fuel Performance Experiments and Analysis and Computerized Man-Machine Communication, Loen, Norway, 23rd-28th May, 1983.

Risø National Laboratory **Risø - M -** 2409

Risø - M - 2409

Title and author(s)

A Systems Modelling Framework for the Design of Integrated Process Control Systems

Morten Lind

Date December 1983

Department or group

Electronics

Group's own registration number(s)

R-3-83

NKA/LIT-3.2(83)124

pages + tables + illustrations

Abstract

The paper describes a systems modelling methodology, called multilevel flow modelling, or MFM, which aims at describing complex production plants as designs, i.e. as systems having goals, functions and equipment realizing these functions. The modelling concepts are based on thermodynamics and lead to a system description in terms of multiple levels of interrelated mass or energy flow structures. The paper discusses as a basis for the modelling framework the general properties of artifacts or designs, characterizes the complexity of production systems and defines the MFM concepts which allow a consistent specification of goals and functions of these systems as generated in the process design. A modelling example is given and the application of the models for the design of plant control strategies is outlined.

Copies to

Available on request from Risø Library, Risø National Laboratory (Risø Bibliotek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116